

Set Items Description  
S1 15340 CURVE() CRYPTOGRAPH? OR ELLIPTIC OR HYPERELLIPTIC  
S2 426 JACOBIAN  
S3 0 STICKELBERGER  
S4 5 S1 (15N) S2  
File 348: EUROPEAN PATENTS 1978-2004/Apr W01  
(c) 2004 European Patent Office  
File 349: PCT FULLTEXT 1979-2002/UB=20040408, UT=20040401  
(c) 2004 WIPO/Univentio

01143508

Method of digital signature, and secret information management method and system

Verfahren zur digitalen Unterschrift und Verfahren und Vorrichtung zur Verwaltung einer Geheiminformation

Procede de signature numerique ainsi que procede et systeme de gestion d'une information secrete

PATENT ASSIGNEE:

Hitachi, Ltd., (204151), 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)

INVENTOR:

Miyazaki, Kunihiko, 4-44-23, Higiriyama, Konan-ku, Yokohama-shi, Kanagawa-ken, (JP)

Takaragi, Kazuo, 3-14-28-305, Kokubuminami, Ebina-shi, Kanagawa-ken, (JP)

LEGAL REPRESENTATIVE:

Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 998074 A2 000503 (Basic)

APPLICATION (CC, No, Date): EP 99121598 991029;

PRIORITY (CC, No, Date): JP 98309936 981030; JP 99241905 990827

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/32

ABSTRACT EP 998074 A2

A method of digital signature for generating a digital signature A that uses a private key d for a message M in which k pieces of numerical information  $u_1, u_2, \dots, u_k$ ) satisfying  $d = f_1(u_1, u_2, \dots, u_k)$  are distributed into and retained by k computers; with regard to each computer of the k computers, a piece of numerical information  $u_i$ ) ( $1 \leq i \leq k$ ) retained by itself, a piece of numerical information  $s_i$ ) generated by itself, and information obtained from pieces of numerical information generated respectively by the computers other than itself by themselves, are made to act on the message M, by that computer, to generate a partial signature  $a_i$ ) on the message M; and partial signatures  $a_i$ ) ( $1 \leq i \leq k$ ) generated respectively by the k computers are used to generate the digital signature A that uses the private key d for the message M.

ABSTRACT WORD COUNT: 148

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 000503 A2 Published application without search report

LANGUAGE (Publication, Procedural, Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200018	1239
SPEC A	(English)	200018	22286
Total word count - document A			23525
Total word count - document B			0
Total word count - documents A + B			23525

...SPECIFICATION the discrete logarithm problem on another group such as a multiplicative group of a finite field, a jacobian group on a hyperelliptic curve, a jacobian group on a Cab curve, or the like.

Further, the above embodiments have been described taking the...

4/5,K/3 (Item 3 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

01062592 . . .  
A network system using a threshold secret sharing method  
Netzwerksystem unter Verwendung eines Verfahrens zur Rückgewinnung eines  
verteilten Geheimnisses mit Schwellwert  
Systeme de reseau utilisant un procede de recuperation a seuil d'un secret  
partage

PATENT ASSIGNEE:

Hitachi, Ltd., (204151), 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo  
101-8010, (JP), (Applicant designated States: all)

INVENTOR:

Miyazaki, Seiji, 59-2-B407, Ontacho-1-chome, Higashimurayama-shi, (JP)  
Takaragi, Kazuo, 14-28-305, Kokubuminami-3-chome, Ebina-shi, (JP)

LEGAL REPRESENTATIVE:

Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538  
Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 936776 A2 990818 (Basic)  
EP 936776 A3 021113

APPLICATION (CC, No, Date): EP 99102090 990202;

PRIORITY (CC, No, Date): JP 9831636 980213

DESIGNATED STATES: DE; FR; GB.

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/30

ABSTRACT EP 936776 A2

In a data encryption/decryption method including an encryption step and a decryption step. In the encryption step (Fig. 2), there are prepared n pairs of secret keys (d1 to d4) and public keys (Q1 to Q4) in a public-key cryptographic scheme, where n is a positive integer. A new key is generated in accordance with at least one of the public keys. Data is encrypted in a common-key cryptographic scheme by use of the new key. There is prepared a (k,n) threshold logic (k is an integer equal to or less than n) having terms associated with the new key and the n public keys. A calculation of the threshold logic is conducted by use of the new key and the n public keys, and encrypted data and a result of the calculation of the threshold logic are stored. In the decryption step (Fig. 3), the new key is restored from k secret keys selected from the n secret keys and the stored result of the threshold logic calculation in accordance with a threshold reverse logic corresponding to the threshold logic and stored data is decrypted by the restored key in the common-key cryptographic scheme.

ABSTRACT WORD COUNT: 196

NOTE:

Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):

Search Report: 021113 A3 Separate publication of the search report  
Application: 990818 A2 Published application without search report  
Examination: 030212 A2 Date of request for examination: 20021212  
Examination: 030502 A2 Date of dispatch of the first examination  
report: 20030317

LANGUAGE (Publication, Procedural, Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9933	1304
SPEC A	(English)	9933	4256
Total word count - document A			5560
Total word count - document B			0
Total word count - documents A + B			5560

...SPECIFICATION elliptic curve cryptosystem, there may be utilizes a cryptosystem using one of other group structures, specifically, the Jacobian group of a hyperelliptic curve or a CAB)) curve, a subgroup of the Jacobian group, and a subgroup of an integral ring.

While the present invention has been described with reference...

00798806

**METHOD FOR MULTIPLYING DIVISOR CLASSES WITH A SCALAR**

**PROCEDE DE MULTIPLICATION DE CLASSES DE DIVISEURS AVEC UN SCALAIRES**

**VERFAHREN ZUM MULTIPLIZIEREN VON DIVISORENKLASSEN MIT EINEM SKALAR**

Patent Applicant/Assignee:

SIEMENS AKTIENGESELLSCHAFT, Wittelsbacher Platz 2, 80333 Munchen, DE, DE  
(Residence), DE (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

GUNTHER Christian, Gustav-Heinemann-Ring 84, 81739 Munchen, DE, DE  
(Residence), DE (Nationality), (Designated only for: US)

Legal Representative:

SIEMENS AKTIENGESELLSCHAFT (commercial rep.), Postfach 22 16 34, 80506  
Munchen, DE,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200131435 A2-A3 20010503 (WO 0131435)

Application: WO 2000DE3750 20001024 (PCT/WO DE0003750)

Priority Application: DE 19952028 19991028

Designated States: CA CN JP US

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Main International Patent Class: G06F-007/72

Publication Language: German

Filing Language: German

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 3873

**English Abstract**

The invention relates to a method for the multiplication of divisor classes with a scalar ( $m$ ), whereby the scalar ( $m$ ) is a whole number and the divisor class is an element of the Jacobian variety of a hyperelliptic curve ( $C$ ) on a finite body ( $F^{2^n}$ ) ( $d$  is in)  $J^{2^n}C(F^{2^n})$ ,  $C: v^{2+uv=u^{5+u^{2+1}}}$ . The inventive method is based on Frobenius endomorphism, whereby a very short tau-adic expansion is obtained enabling rapid calculation of multiplication.

**French Abstract**

La presente invention concerne un procede de multiplication de classes de diviseurs avec un scalaire ( $m$ ), dans lequel le scalaire ( $m$ ) est un nombre entier et la classe de diviseurs est un element de la variete jacobienne d'une courbe hyperelliptique ( $C$ ) sur un corps infini ( $F^{2^n}$ ) ( $d$  is in)  $J^{2^n}C(F^{2^n})$ ,  $C: v^{2+uv=u^{5+u^{2+1}}}$ . Le procede de l'invention repose sur l'endomorphisme de Frobenius, ce qui permet d'obtenir une tres courte expansion tau qui permet un calcul rapide de la multiplication.

**German Abstract**

Die Erfindung betrifft ein Verfahren zur Multiplikation von Divisorenklassen mit einem Skalar ( $m$ ), wobei der Skalar ( $m$ ) eine ganze Zahl und die Divisorenklasse Element der jacobischen Varietät einer hyperelliptischen Kurve ( $C$ ) über einem endlichen Körper ( $F^{2^n}$ ) ist ( $d$  is in)  $J^{2^n}C(F^{2^n})$ ,  $C: v^{2+uv=u^{5+u^{2+1}}}$ . Das erfindungsgemäße Verfahren beruht auf dem Frobenius-Endomorphismus, wobei durch einen Rundungsschritt eine sehr kurze tau-adische Expansion erhalten wird, die eine schnelle Berechnung der Multiplikation erlaubt.

**Legal Status (Type, Date, Text)**

Publication 20010503 A2 Without international search report and to be republished upon receipt of that report.

Examination 20010802 Request for preliminary examination prior to end of 19th month from priority date

Search Rpt 20011025 Late publication of international search report

Publication 20011025 A3 With international search report.

English Abstract

...whereby the scalar (m) is a whole number and the divisor class is an element of the Jacobian variety of a **hyperelliptic** curve (C) on a finite body ( $F^{2 \times n}$ ) ( $d \in \text{in}^J \subset C$ ...)

4/5,K/5 (Item 2 from file: 349)

DIALOG(R) File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00500681 \*\*Image available\*\*

**MEASURING POSITION AND ORIENTATION USING MAGNETIC FIELDS**

**MESURE DE POSITION ET D'ORIENTATION AU MOYEN DE CHAMPS MAGNETIQUES**

Patent Applicant/Assignee:

CORMEDICA CORPORATION,

Inventor(s):

SCHNEIDER Mark R,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9932033 A1 19990701

Application: WO 98US13431 19980630 (PCT/WO US9813431)

Priority Application: US 97996125 19971222

Designated States: CA IL JP MX AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC  
NL PT SE

Main International Patent Class: A61B-005/05

Publication Language: English

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 15378

English Abstract

A method, and apparatus for, determining the position, orientation of a remote object relative to a reference coordinate frame that includes a plurality of field generating elements (11-18) for generating electromagnetic fields, a drive (71-78) for applying to the generating elements, signals that generate a plurality of electromagnetic fields that are distinguishable from one another, a remote sensor (20) having one or more field sensing elements for sensing the fields generated, a processor (50) for processing the outputs of the sensing element(s) into remote object position, and orientation relative to the generating element reference frame.

French Abstract

Procédé et dispositif servant à déterminer la position et l'orientation d'un objet à distance par rapport à un cadre de coordonnées de référence comprenant une pluralité d'éléments (11) (18) servant à générer des champs électromagnétiques, un circuit d'attaque (71) (78) servant à appliquer à ces éléments des signaux générant une pluralité de champs électromagnétiques distincts les uns des autres, un détecteur à distance (20) possédant un ou plusieurs éléments servant à détecter les champs générés et un processeur (50) servant à traiter les sorties des éléments de détection afin de les convertir en position et en orientation d'objet à distance en fonction du cadre de référence des éléments de génération.

Fulltext Availability:

Detailed Description

Detailed Description

... section).

18

Exact calculation of the Jacobian and/or Hessian can be accomplished using symbolic software. The **Jacobian** and Hessian for the circular coils, however, require further evaluations of the **elliptic** integrals. While it is not my intent to teach others about solving non-linear systems of equations...